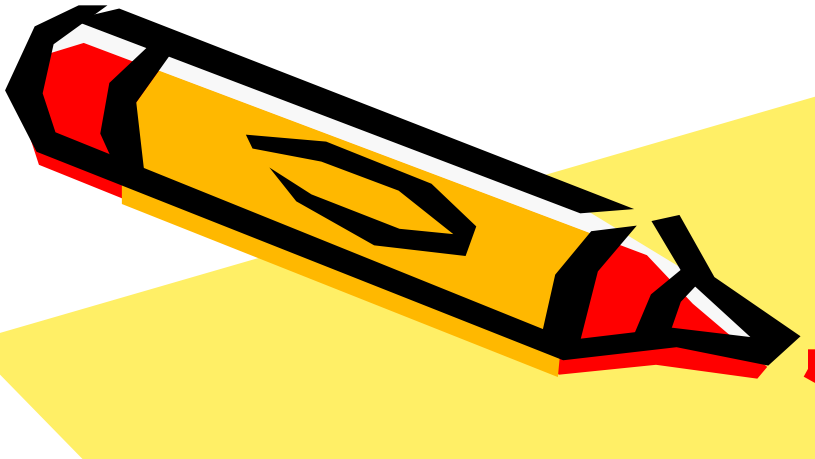


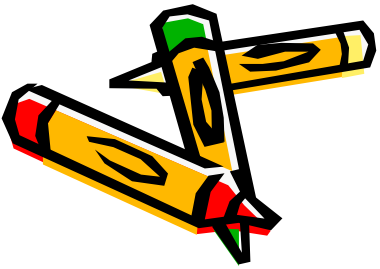
Introduction To:

Information Assurance for Security Managers

Points of Contact

Information Assurance Manager's Office

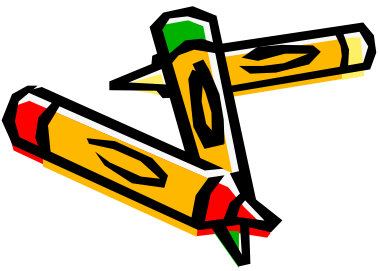
- **James "Jim" Preston - 526-0565**
  Jim.Preston@carson.army.mil
- **Cindy Thornburg - 526-1386**
  Cindy.Thornburg@carson.army.mil
- **Henry Felch - 526-8985**
  Henry.Felch@carson.army.mil
- **Gwendolyn Phillips - 526-4596**
  Gwendolyn.Phillips@carson.army.mil



Points of Contact

Information Assurance Manager's Office

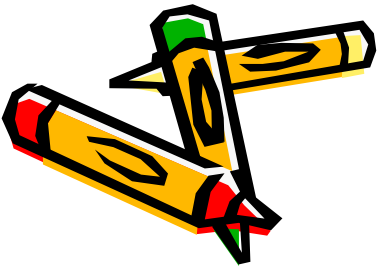
- **Patty Harden – 524-4541**
  Patty.Harden@carson.army.mil
- **Mark Saunders – 524-0588**
  Mark.Saunders@carson.army.mil
- **Ray Hand – 526-3965**
  Ray.Hand@carson.army.mil
- **Chuck Clark – 526-5510**
  Charles.Clark@carson.army.mil



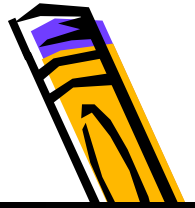
Cyber Battlespace

Subject Outline

- Introduction and IA Goals
- Why and References
- Accreditation and Duties = DITSCAP
- Information Technology levels (ADP)
- Current events and Video
- IAVA & Scanning Tools
- Policies
- Reporting Security Incidents and Virus
- INFOCON and SIPRNET
- Network Security, PKI
- Websites and Handouts

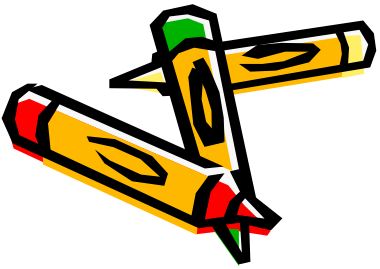


IA GOAL



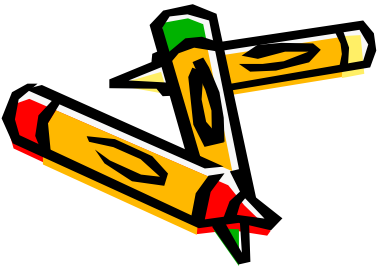
Why

- To ensure the integrity, confidentiality, availability and non-repudiation of data
- To identify and authenticate the user of the data
- Create a level of trust by establishing across the board policies to protect computer systems and associated data while in transit, garrison, and deployed.
- The computer network is now a force multiplier and organizational asset.
- Public Law 100-235, AR 25-2



Stumbling Blocks to Security

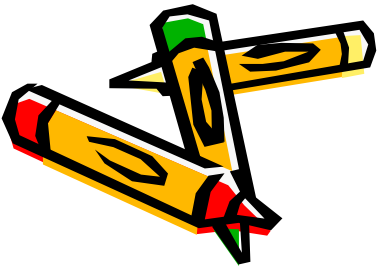
- Users: Using short cuts, social engineering, forgetting they are on a dot mil network
- Management: Not wanting to enforce policy, not understanding the threat
- Software: Weak code, vulnerabilities
- Hardware: Accessibility
- Security: Information overload



Security Threats from E-mail

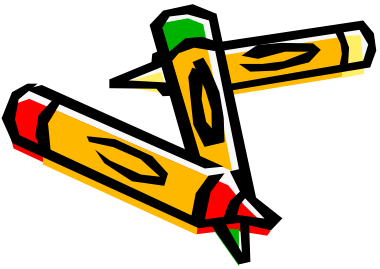
- Executable file in attachments
- Macro, Worms and Trojans
- Internal Users going to their ISP accounts: leaving a connection open
- Not digitally signing sensitive emails or understanding how

If you would not send the information on a post card, do not send it by email



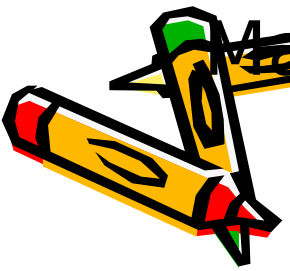
Reasons Cited for Security Violations

- Weak passwords: Not as much now
- Write down passwords: most common
- Users do not take problem seriously
- User leaves system logged on but not locked
- Unauthorized software
- No one likes controls



References

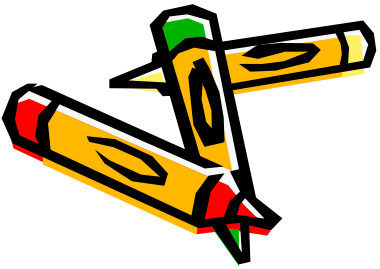
- AR 380-5 Information Security
- AR 380-53 Information Security Systems Monitoring
- AR 380-67 Personnel Security Program
- DOD 8500.1 Information Assurance
- DOD 8500.2 Information Assurance Implementation
- AR 25-1 Army Information Management
- AR 25-2 Information Assurance (primary)
- FC 25-1 Fort Carson Information Management



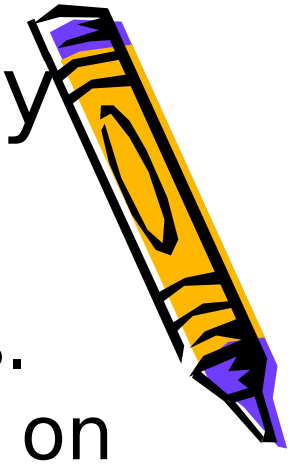
Questions

Accreditation of Information Technology

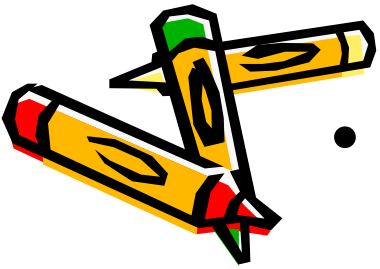
- DoD Information Technology Security Certification and Accreditation Process = DITSCAP
- WHO = Prepares Accreditation, IMO, IASO, SM
- WHAT= All Computer Systems, including Tactical Systems, Classified Systems and stand alone.
- WHEN= Before systems are used or connected to the network
- HOW= AR 25-2, DoD 8510.1-M
- Fort Carson's template available on IA website http://carsweb.carson.army.mil/doim/ia/



Information Assurance Security Officer (IASO)



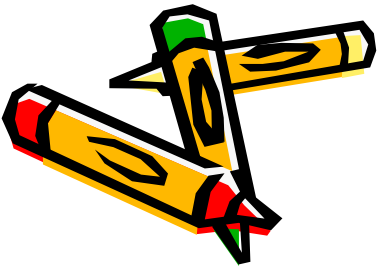
- The IASO is appointed on orders.
- There are 13 major duties listed on page 12, AR 25-2 (para 3-2, f, 1-13).
- The IASO is responsible for the accreditation of information systems (IS).
- Ensure implementation of IA policy, guidance, and training requirements.
- Level 1 training within 6 months after appointment. Training found at: **http://ia.gordon.army.mil/iaso/default.htm**
- Must be registered in A&VTR



Critical Components

Security Manager's responsibilities

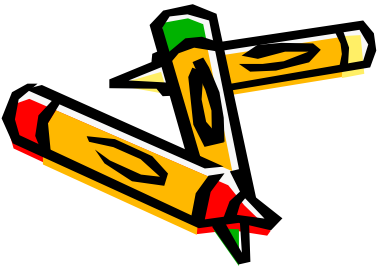
- The Security Manager is appointed on orders.
- Responsible to assess security violations
- Coordinate with IASO and IMO on DITSCAP and risk assessment
- Command Inspections and Security Manager Inspection point of contact



Questions

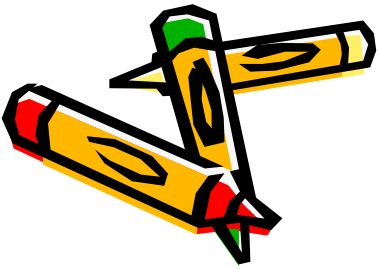
Information Technology Level (ADP) AR 25-2 and AR 380-67

- **Investigation vs. Clearance**
- Three Levels
  - I: classified (SA/NA)
  - II: limited privileges (IMO)
  - III: user
- Contractors, Consultants and all DoD persons will meet the AR 380-67 standard.
- No password or access to the Network without **completed favorable background** investigation.
- An interim can be granted until the investigation is completed



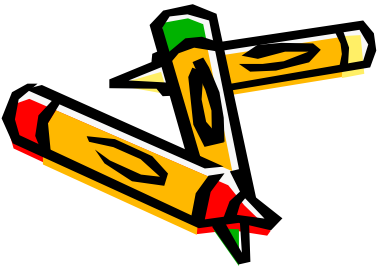
Interim approval for Network Access

- Proof that all paperwork has been submitted for the investigation and the investigation has been open
- Favorable local records check
- Letter from 1st 05 or above in charge of command requesting the approval
- All information goes through IA to the DAA for approval



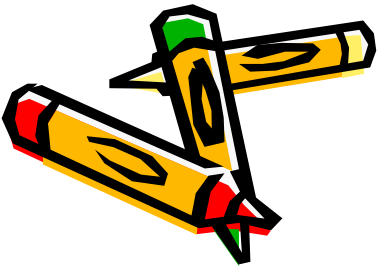
Current Events
Social Engineering 101

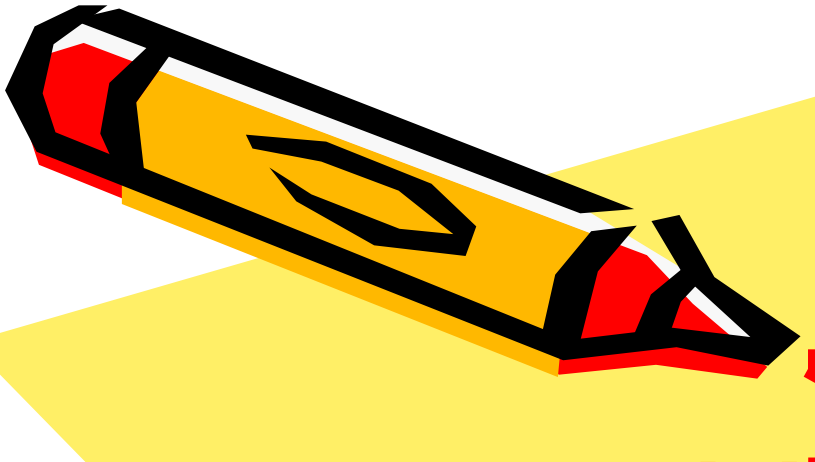
- Still applies today, even more so
- Verifying workers credentials and watching what they are doing
- Credit Card receipts should be checked to ensure the account number is blank out
- Check Credit Card to ensure that it is yours



Current Events

- Logging into the computer to help out other soldiers
  - If they surfing under your log on you are still responsible
- Users leaving IE up and running thus coming up as the number one user on the smart filter





Video

Access Denied

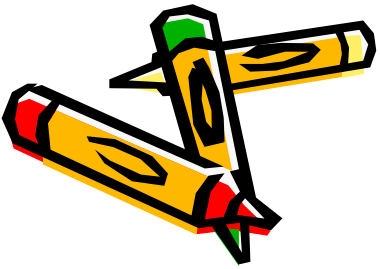
Computer Crime:Deter, Detect, Defend

Questions

"I swear to you the mouse
was this fricken big!!!"

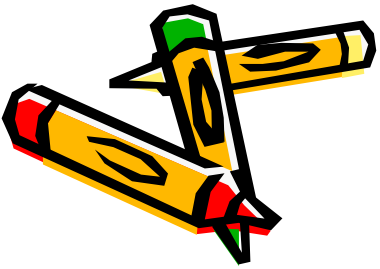
IAVA

- Information Assurance Vulnerability Alert (IAVA)
- Issued on behalf of the Army CIO/G6 and Army G3
- Vice Chief of Staff Army states that IAVA compliance is a Force Protection Issue and a Commanders Responsibility. (MSG DACS-ZB/160453Z Jan 04)
- Compliance is Mandatory



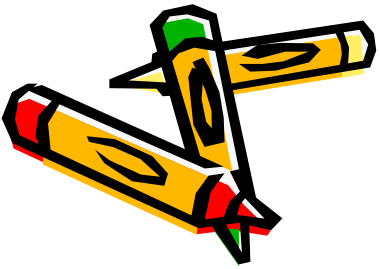
IAVA

- IAVA Message contains:
  - Suspense date
  - List and description vulnerability or problem
  - Lists specific actions to correct vulnerability or problem
- ACERT must approve all extensions



A&VTR

- Asset and Vulnerability Tracking Resources
- Located at https://newia.us.army.mil/modules
- A&VTR is a tool to gather and consolidate IAVA reporting and training
- All assets must be registered in A&VTR
- Assign primary and alternate POC for each asset
- Assets have been entry using HARRIS Stat



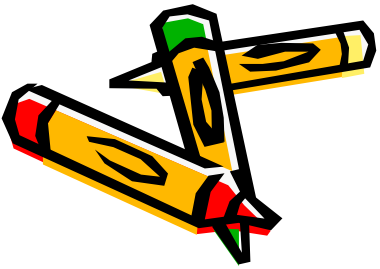
IA Scanning tools

- ISS System Scanner
  - Requires Agent
  - Servers
- ISS Internet Scanner
  - Requires only a connection to the network
  - Identification of network assets
  - Identify/Verify vulnerabilities
- Harris STAT Scanner
  - Requires Local Admin Rights
  - IAVA Compliance
- Testing Retina

Questions

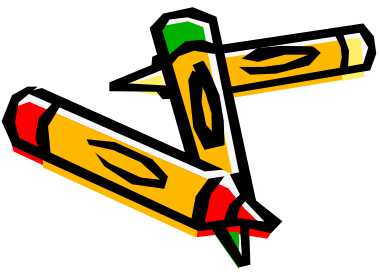
Army Policies

- On training
  - User
  - IASO
  - SA
- E-mail Accounts
  - Investigation
  - Password length
- Web pages
  - Public Release (PAO)
  - SAEDA
  - FOIA
  - OPSEC



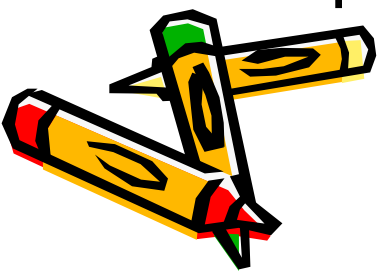
USER Responsibilities on the Network

- Internet Accounts
- Decorum
- Misuse
  - pornography
  - business
  - chain letters
- Official Duties
- Not-to-interfere with
- Contacting Media
- Congressional
- Official Information
- Copyright
- Privacy Act
- Collection
- Eavesdropping
- Recordkeeping

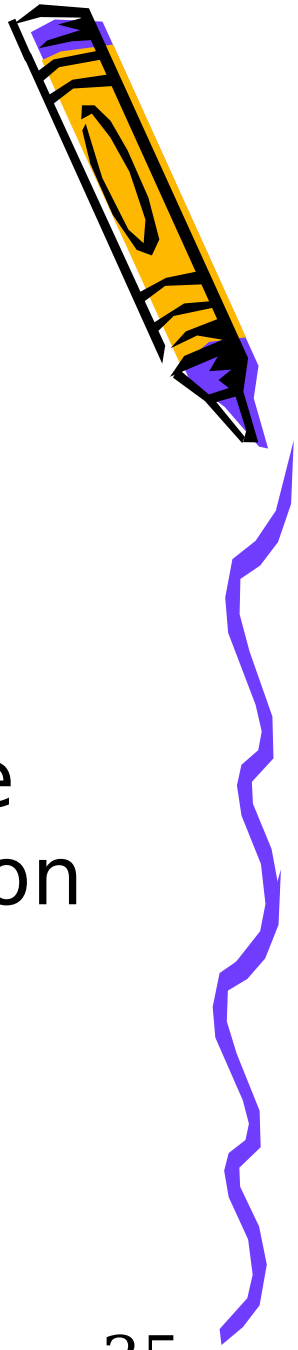


Authorized Software

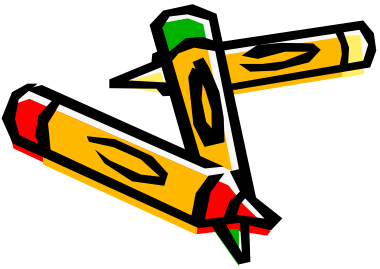
- Most software is included in an Enterprise Software Contract/Agreement. Such as the Operating System, Microsoft Office, Norton
- Networthiness certificate for specialized programs.
- Non-standard software must be approved by DOIM IA before being loaded on the computer



Unauthorized Software



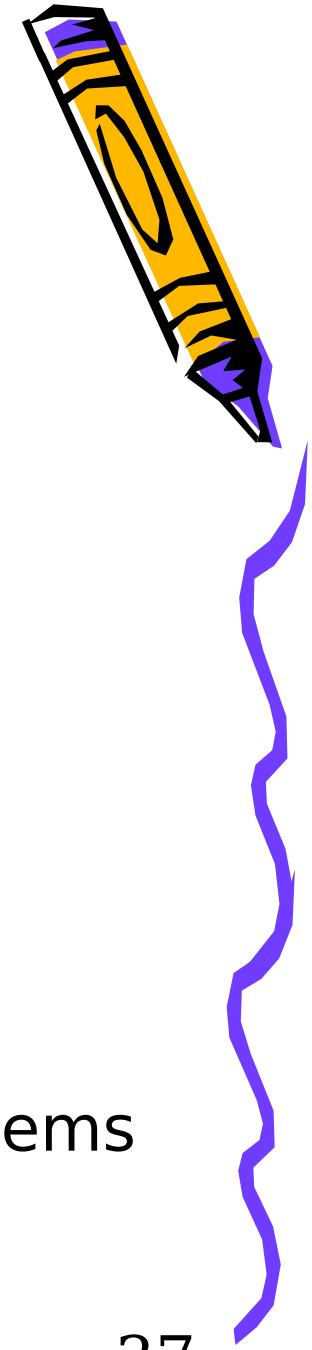
- Any software that negates or circumvents the system security
- Shareware or Freeware unless specifically approved
- Open Source software when source code is not available for examination
- Peer to Peer Software (P2P)



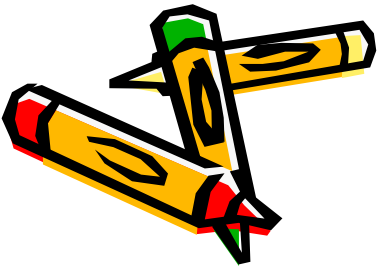
Information Systems Security Incidents

- Always report incident to IA Office.
- Initial notification will be within first 24 hours: who, what, where, when, action taken and point of contact.
- Major types of activities that must be reported, AR 25-2 page 36 (para. 4-21 c1-8, d1-5)
- All incidents will be investigated.

Information Systems Security Incidents

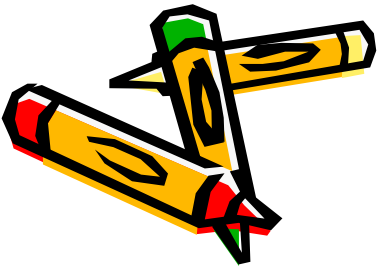


- Suspected or known Intrusions
- Unauthorized access to data
- Indications of unauthorized user access
- Unexplained modifications of data/write
- Unrequested output
- Inconsistent markings
- Abnormal system response
- Malicious software --- viruses
- Alerts by Network Intrusion Detection Systems



Basic Steps to Take if You Think You Have a Virus

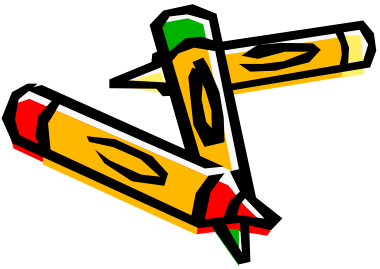
- Stop work
- Unplug the network cord from the wall
- Do NOT power down the computer
- Note- your location - LAN/remote/desk
- Call –IASO/SM, IMO, DOIM- Help Desk (6-2270)



Questions

Information Condition INFOCON

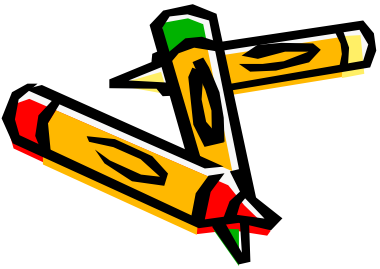
- Information Operation Conditions
- Its an alert system
- Five levels: Normal, alpha - delta
- Network-centric environment
- Increase in condition - do not have to meet all criteria



SIPRNET

- Memorandum signed by O-6 requesting service and providing funds

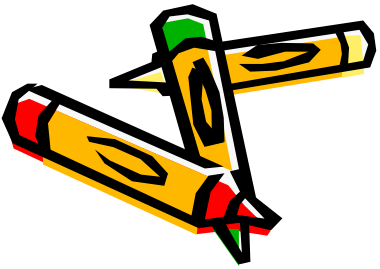
- Requires DITSCAP/Risk package approval **before** activation/connectivity
  - Open storage letter
  - SOP with Annex A, B, C
  - Orders for IASO
  - IASO certificate



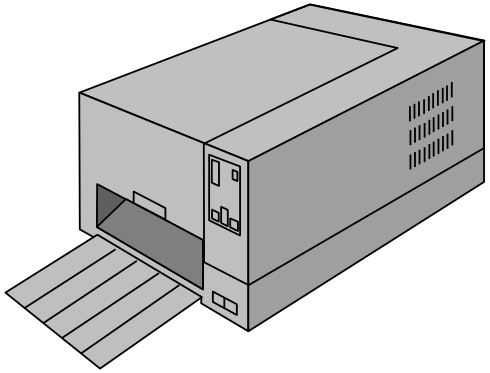
SIPRNET ACCOUNT

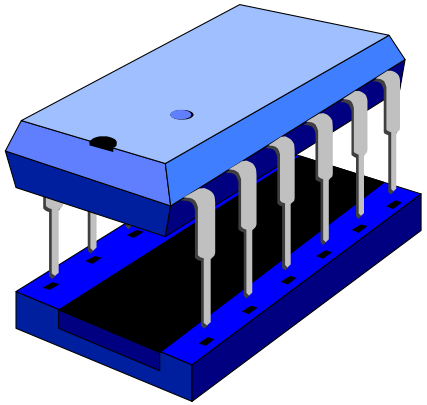
- Submit to Help Desk
- FC Form 1001-E
  - Type in NATO and date it occurred
- Attached the following checks
  - DCII or JPAS printout (less then 30 days old)

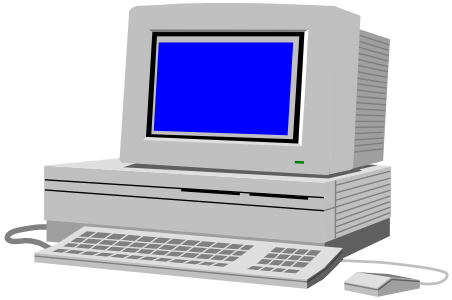
  Local & NCIC check (FC Form 18E) (less then 30 days old)

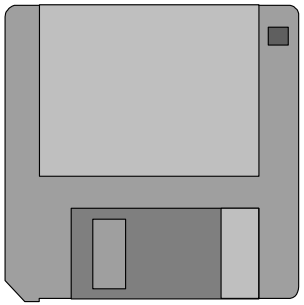


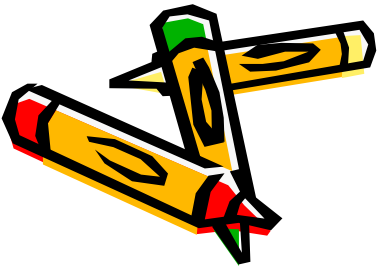
Declassification of:
SCI -- Collateral -- SBU









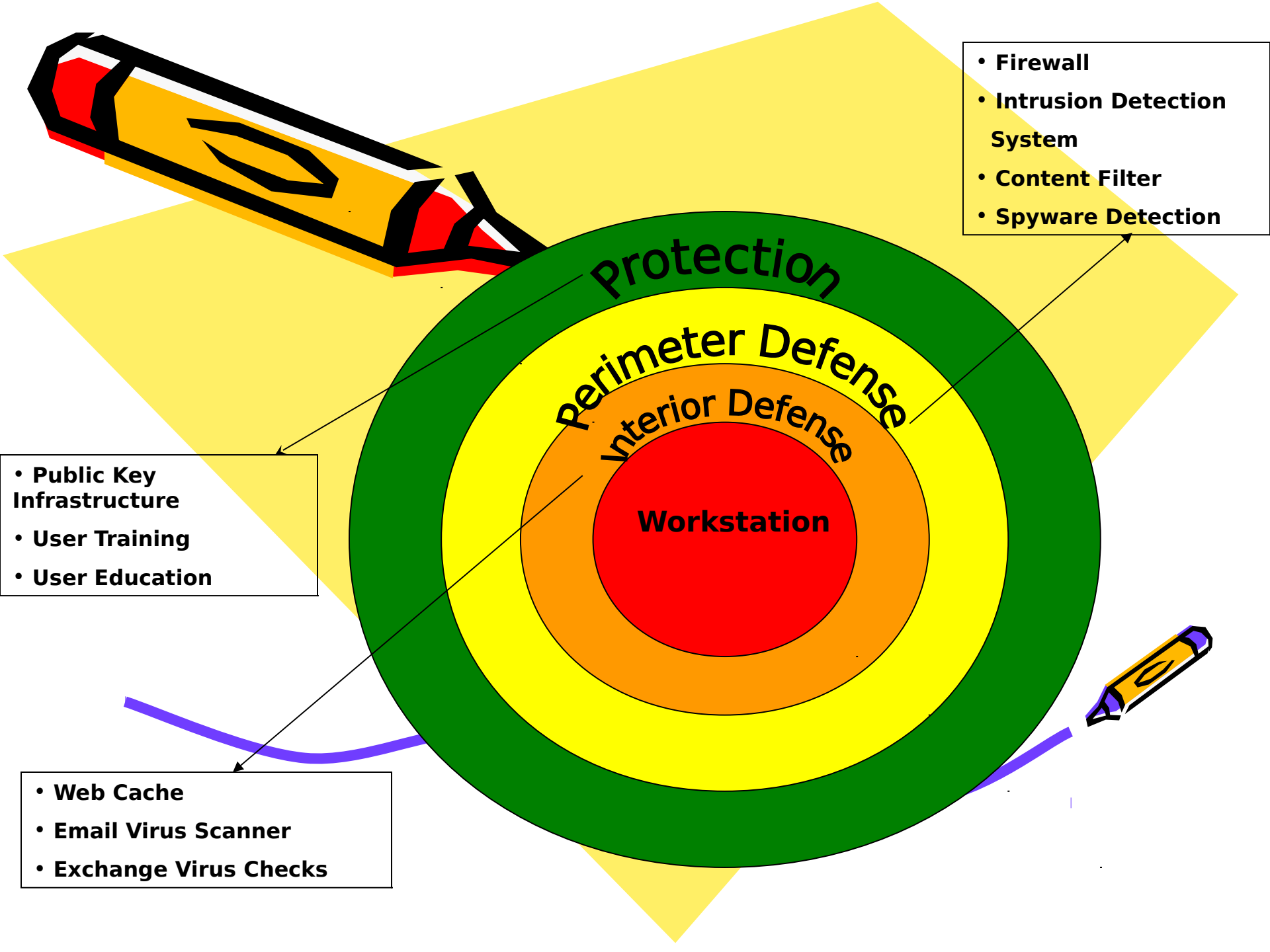


- Declassification
- Sanitization
- Wiping

- **A device is never declassified**

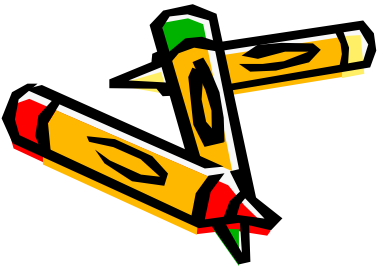
.

Questions

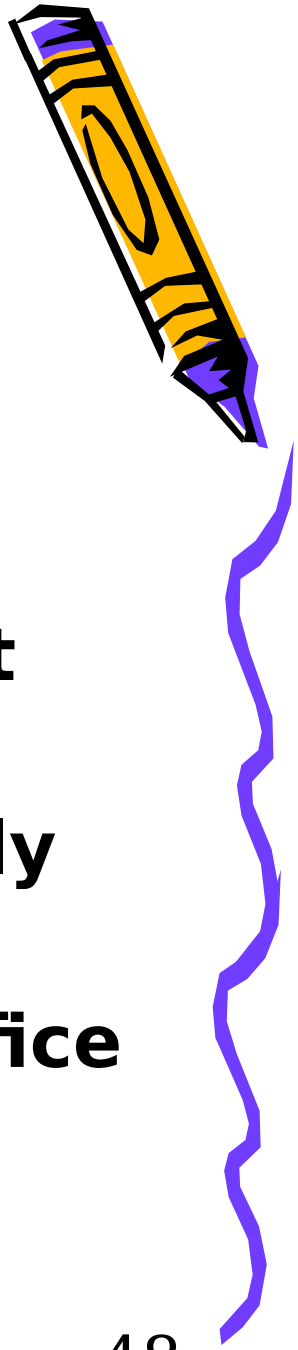

• Firewall
• Intrusion Detection System
• Content Filter
• Spyware Detection
Protection
Perimeter Defense
Interior Defense
Workstation
• Public Key Infrastructure
• User Training
• User Education
• Web Cache
• Email Virus Scanner
• Exchange Virus Checks

2004 Problems

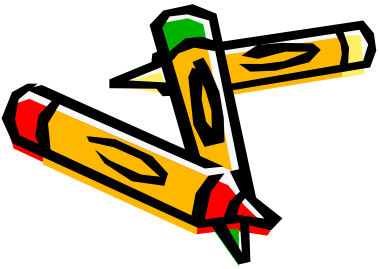
- Buffer over flows
- Super Worms, RPC, DCOM, NETSKY, MYDOOM
- Identifying owners of systems
- E ARMY U and Personal computers on the network.
- Personal firewalls
- IRC and P2P



How To Keep Up

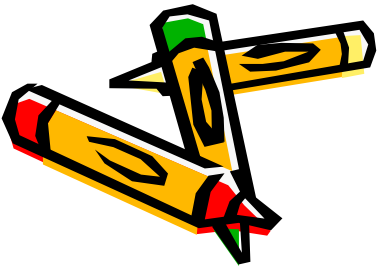


- **Baseline your environment: (computer managed by DOIM's endpoint)**
- **Bring everything up-to-date that you can (operating system XP)**
- **Accreditation Standards – Comply & updated as they occur**
- **Communicate with DOIM's IA Office**



PKI/CAC

- New ID Card for all users
  - REMEMBER PIN
  - Pin can be reset without getting new ID card
- Installation of
  - Card readers
  - Middleware (NetSign)
- Must sign all sensitive emails and encrypt email dealing with Global War On Terrorism



Website

The Army IA website is:

https://informationassurance.us.army.mil

Fort Gordon website is:

http://ia.gordon.army.mil/ia_courses.htm

Information Assurance Support Environment

http://iase.disa.mil

Fort Carson's Intranet site:

http://www.carson.army.mil/doim/ia